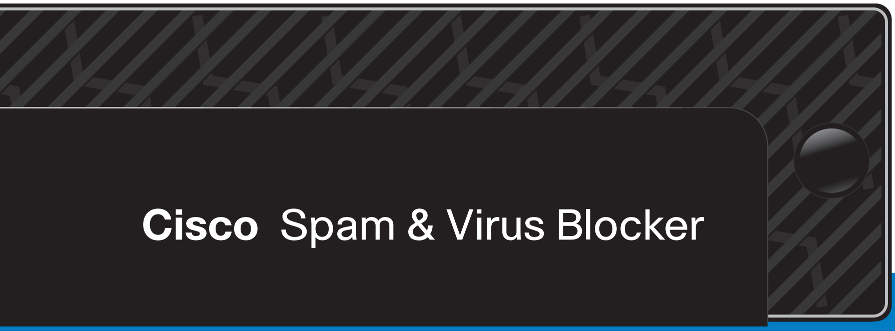


Cisco Spam & Virus Blocker

QUICKSTART GUIDE

1 Getting Started

You will need the following items to get started:

- A desktop or laptop computer
- Two ethernet cables (one ethernet cable is shipped with the Blocker, and you must provide the second).
- Web browser
- Network information for “Go Live” configuration (Step 10):
  - MX records. Determine where your current MX records point.
  - NAT settings. Determine where your Port 25 traffic is sent.
  - Firewall settings. Determine the firewall ports you may need to open.

Before you begin, write down the following information about your network and administrator settings. You will need to enter this information when running the System Setup Wizard, starting on Step 8.

NETWORK SETTINGS

Blocker Hostname ______________________

Blocker IP Address______________________

Subnet Mask ______________________

Gateway IP Address ______________________

LOCAL DNS SERVER INFORMATION

Primary DNS Server IP Address______________________

Secondary DNS Server IP Address______________________

MAIL CONFIGURATION SETTINGS

Accept email for the following domains ______________________

Mail Server______________________

ADMINISTRATOR SETTINGS

Administrator Email ______________________

Administrator Username admin (non-configurable)

Administrator Password ______________________

in the box

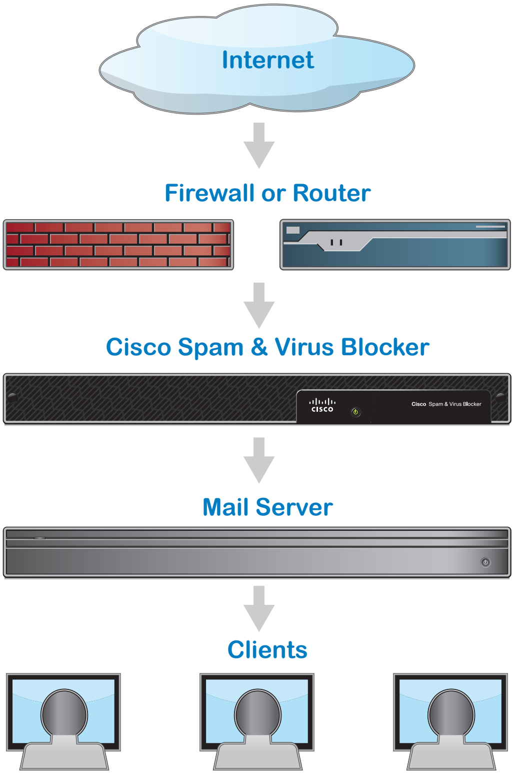
Cisco Spam & Virus Blocker • 1 Ethernet Cable
Quickstart Guide • FAQ
Rail Kit • T-Shirt • Documentation CD

Plan the Installation

2

To detect spam and viruses, the Cisco Spam and Virus Blocker Blocker must be installed at the perimeter of your network. It needs to be the first machine with an IP address that can access the Internet.

Plan for your network configuration to look something like this:



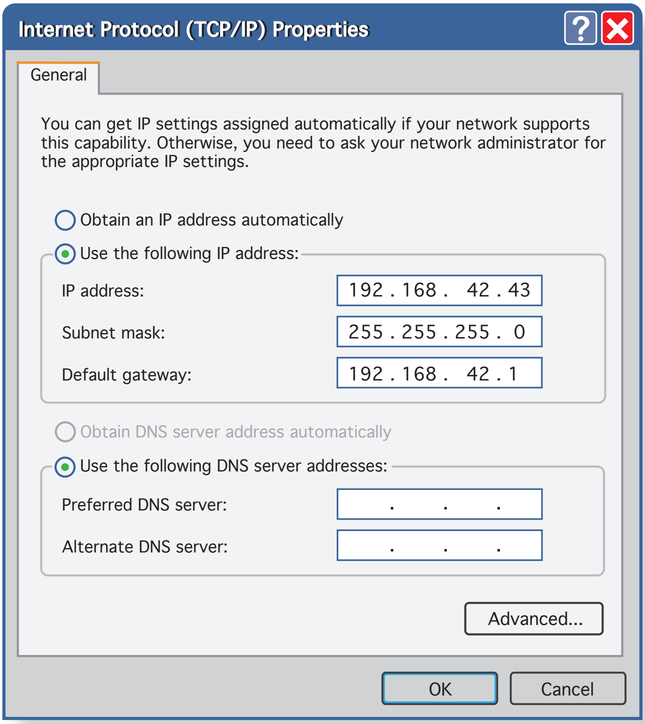
3 Change Your IP Address

To connect to the Blocker, you will need to temporarily change the IP address of your computer.

First, make a note of your current IP configuration settings as you will need to revert to these settings later.

Then, make the following changes to your IP address:

- IP Address: 192.168.42.43
- Subnet Mask: 255.255.255.0
- Gateway: 192.168.42.1



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 42 . 43

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 42 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

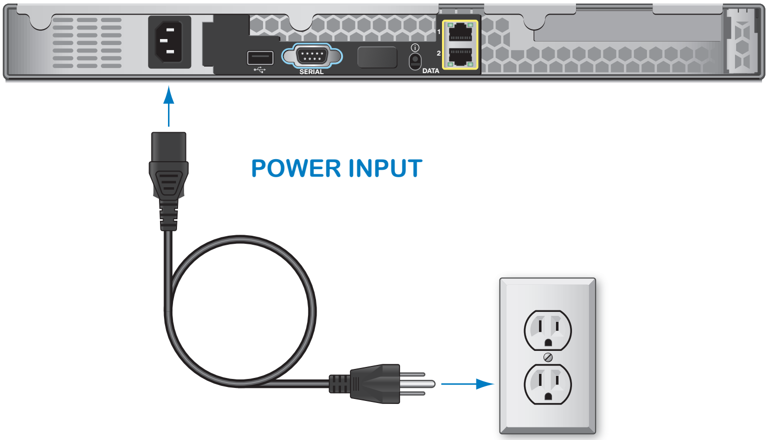
Alternate DNS server: . . .

FOR MORE **info**

On changing your IP address in a Windows or Mac environment, see **Appendix A.**

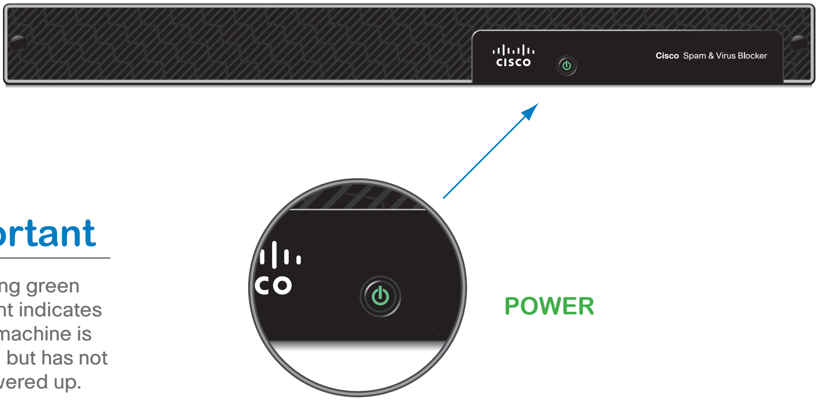
Plug In 4

Place the Blocker in a location that provides enough air flow to prevent overheating.



Plug the Blocker's power cable into an electrical outlet.

5 Power Up



important

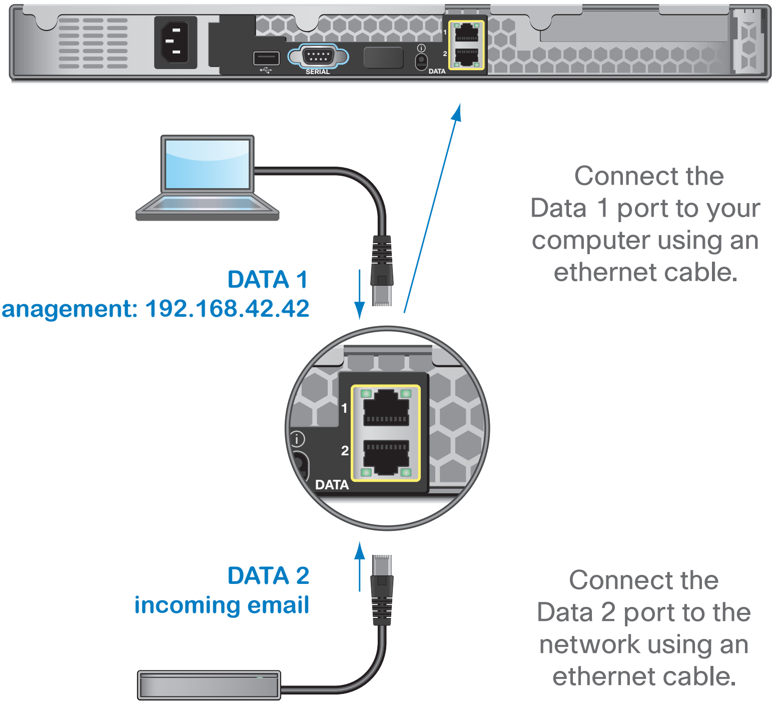
A flashing green power light indicates that the machine is plugged in but has not yet powered up.

Power up by pressing the On/Off switch on the front panel of the appliance. After the machine powers up, a solid green light indicates that the machine is running.

WAIT 5 MINUTES

Connect to the Blocker 6

The Blocker has two network ports: Data 1 and Data 2.



Connect the Data 1 port to your computer using an ethernet cable.

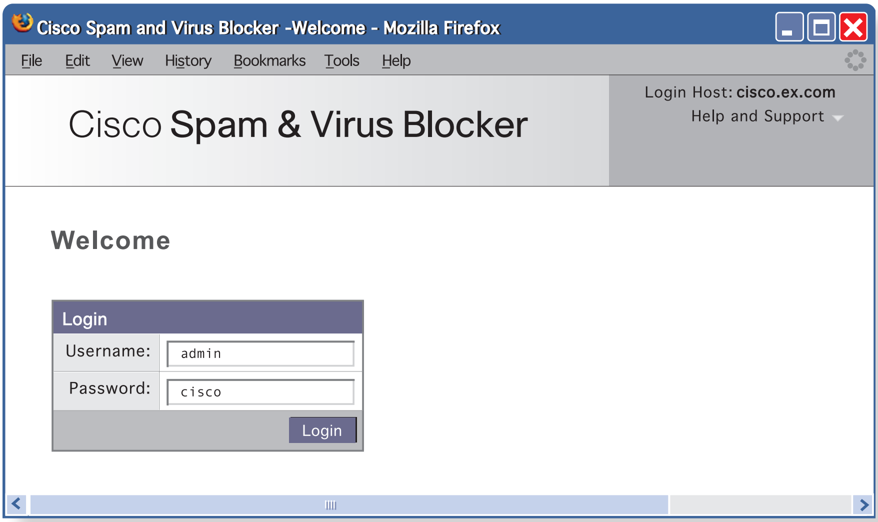
Connect the Data 2 port to the network using an ethernet cable.

For the purposes of setup, connect to Data 1 as your management interface and configure incoming email on the Data 2 interface.
You can change these settings after the initial installation if you wish.

7 Log on to the Blocker

Go to your management interface by entering the following URL in a web browser: http://192.168.42.42

The login page for the Blocker opens.


Cisco Spam and Virus Blocker -Welcome - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
Cisco Spam & Virus Blocker
Login Host: cisco.ex.com
Help and Support

Welcome

Login

Username: admin

Password: cisco

Login

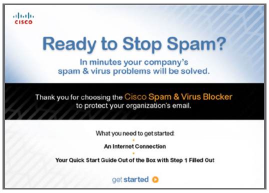
Enter the following login information:

- Username: admin
- Password: cisco

Run the System Setup Wizard

8

The System Setup Wizard starts automatically.



Ready to Stop Spam?

In minutes your company's spam & virus problems will be solved.

Thank you for choosing the Cisco Spam & Virus Blocker to protect your organization's email.

What you need to get started:

- An Internet Connection
- Your Quick Start Guide Out of the Box with Step 1 Filled Out

Accept **license**.

Enter **registration** information.

Enter **network** information (gathered in Step 1).

Set anti-spam and anti-virus **security** settings.

Review the configuration summary page.

Log back in to the appliance with the username ***admin*** and the new password you set in the System Setup Wizard.

The Blocker uses a self-signed certificate that may trigger a warning from your web browser. You can simply accept the certificate and ignore these warnings.

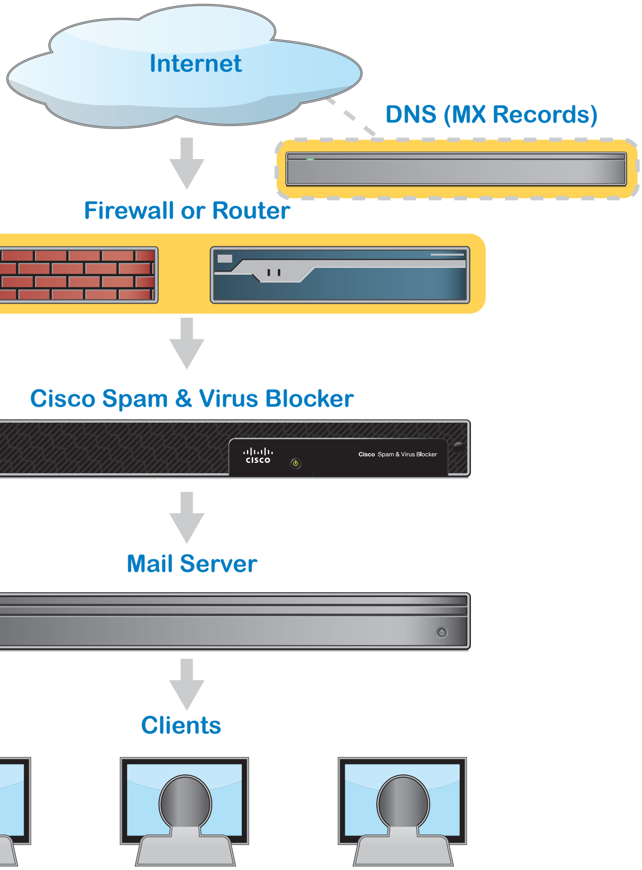
Don't forget to write down your new administrator password and keep it in a safe place!

9 Go Live

Almost there....

You have completed the Blocker configuration. Now, you need to make changes in your network environment to 'go live' and allow the Blocker to process email.

The following data flow diagram highlights network settings that you may need to change.



Configure Network Settings 10

To allow the Blocker to receive email, you may need to change the following network settings:

MX RECORDS

If your MX records point to a mail server, or if your spam and virus solution is hosted, you will need to change your MX records to point to the Blocker. To determine these settings, review your DNS records. Note that it can take up to 72 hours for DNS setting changes to propagate.

FOR MORE info

About your MX records, see **Appendix B.**

PORTS

In your firewall or router, you need to open the following ports:

- **PORT 25.** Ensure that Port 25 is open for inbound and outbound traffic. You must also ensure that Port 25 traffic is directed to the Blocker. To determine your current Port 25 settings, review the port settings on your firewall or router.
- **PORT 80.** Ensure that Port 80 is open for outbound traffic. This port is used to download important updates to your Blocker, such as virus signatures and information about what companies send spam to your network.
- **PORT 443.** Ensure that Port 443 is open for outbound traffic. This port is used to update information about your email traffic to Cisco. The information your Blocker shares with Cisco is used to enhance the algorithms that determine which email is spam and which email is legitimate.

  Important: Port 443 is used to upload registration data and download the permanent feature keys. If you do not open this port, your feature keys cannot be downloaded.

Note: You may need to open other firewall ports in addition to those listed above. Please see “Firewall Information” in the *Cisco Spam & Virus Blocker User Guide.*

FOR MORE info

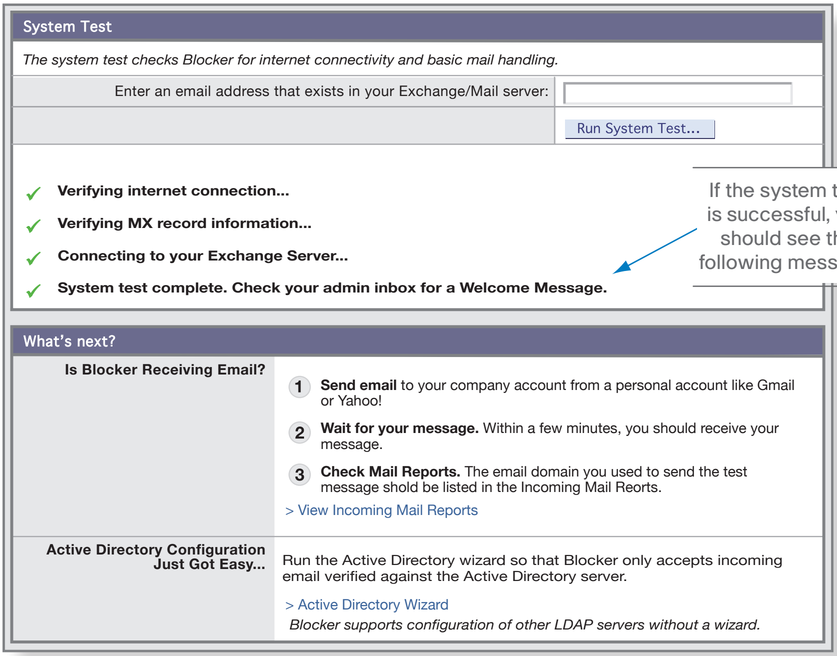
About changing NAT settings, see **Appendix C.**

NAT SETTINGS

If your firewall or router is configured for Network Address Translation (NAT), you need to configure port fowarding. To determine if you need to make changes, review the NAT settings on your router or firewall.

11 Test the Blocker

Use the system test to verify that the Blocker is running properly. On the Next Steps page, enter an email address that is valid in your mail server, and click **Run System Test**.



System Test

The system test checks Blocker for internet connectivity and basic mail handling.

Enter an email address that exists in your Exchange/Mail server:

✓ **Verifying internet connection...**

✓ **Verifying MX record information...**

✓ **Connecting to your Exchange Server...**

✓ **System test complete. Check your admin inbox for a Welcome Message.**

If the system test is successful, you should see the following message.

What's next?

Is Blocker Receiving Email?

1 **Send email** to your company account from a personal account like Gmail or Yahoo!

2 **Wait for your message.** Within a few minutes, you should receive your message.

3 **Check Mail Reports.** The email domain you used to send the test message shold be listed in the Incoming Mail Reorts.

> View Incoming Mail Reports

Active Directory Configuration Just Got Easy...

Run the Active Directory wizard so that Blocker only accepts incoming email verified against the Active Directory server.

> Active Directory Wizard

Blocker supports configuration of other LDAP servers without a wizard.

A successful system test sends a welcome email to the account you entered during the Blocker configuration. Check this account to verify you received the email.

FINAL TEST

Send an email from a private email account (such as Gmail or Yahoo! Mail) to your company email account. Click Monitor > Incoming Mail to check your mail reports. If the Blocker processed the test message, the email domain of your personal email account appears in the Incoming Mail report.

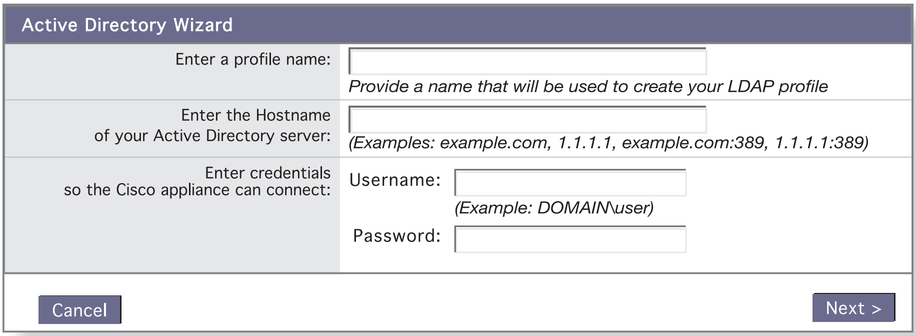
12

Run the Active Directory Wizard (OPTIONAL)

You can run the Active Directory Wizard to enable the Blocker to accept email for users verified against your Active Directory server. This adds another layer of security to your network.

To run the Active Directory Wizard, go to System Administration LDAP. Select the “using Active Directory Wizard” checkbox, and then click **Add LDAP Server Profile**.

Note: You will need the hostname and login information for your Active Directory account to run the Active Directory Wizard.



Active Directory Wizard

Enter a profile name: ______
Provide a name that will be used to create your LDAP profile

Enter the Hostname of your Active Directory server: ______
(Examples: example.com, 1.1.1.1, example.com:389, 1.1.1.1:389)

Enter credentials so the Cisco appliance can connect:
Username: ______
(Example: DOMAIN\user)
Password: ______

Important: As you make configuration changes in the GUI, you must explicitly commit those changes by clicking the **Commit Changes** button. This button appears when you have uncommitted changes that need to be saved.

13 Configuration Summary

Review the following details of your configuration.

MANAGEMENT

You can manage your Blocker from the management port (Data 1) by entering **http://192.168.42.42,** or via the IP address assigned to your Data 2 interface after you have completed the System Setup Wizard. If you reset your configuration to factory default settings (for example, by re-running the System Setup Wizard), you can only access the Management interface from the Data 1 port (http://192.168.42.42), so ensure you have a connection to the Data 1 port.

Also, verify that you open firewall Ports 80 and 443 on your management interface.

INCOMING EMAIL

After running the System Setup Wizard, your Data 2 port is configured for inbound email and management settings are enabled on this interface.

OUTBOUND EMAIL

After running the System Setup Wizard, your Blocker is configured to accept inbound email. You can also configure it to relay outbound email. For instructions on configuring outbound email, see the *Cisco Spam & Virus Blocker User Guide.*

COMPUTER IP ADDRESS

Remember to change your computer IP address back to the original settings that you noted in Step 3.

warning

You must shut down your Blocker from the System Administration > Shutdown/Reboot page to prevent corruption of your queue and configuration files.

You’re Done

Congratulations, you have successfully installed the Cisco Spam and Virus Blocker!

You may want to use message tracking and reporting to better understand how the Blocker is defending your network:

MESSAGE TRACKING

You can view details about message delivery and blocking by running queries using the Message Tracking service (in the GUI). To access message tracking, go to Monitor > Message Tracking.

REPORTING

You can view statistics about spam and virus blocking on your network by viewing reports available in the Email Security Monitor (in the GUI). To access the reporting overview page, go to vMonitor > Overview.

MORE INFORMATION

There are other features you may want to configure for your Blocker. For more information about configuring message tracking and reporting and for details about other available Blocker features, see the Blocker documentation (located on the Documentation CD shipped with your appliance).

You can find electronic versions of user guides or request support by visiting: **http://www.cisco.com/support**

Additional information about the Blocker can be found at:
www.cisco.com/go/blocker

a

Appendix

Changing Your Laptop IP Address (for Step 3)

For Windows

1. Go to the Start menu and click **Control Panel.** The Control Panel opens.
2. Double-click **Network Connections**. The Network Connections window opens.
3. Right-click on the LAN or the correct Local Area Connection, and then click **Properties.**
4. Select **Internet Protocol (TCP/IP)**, and then click **Properties.**
5. Check **Use the following IP Address** and enter 192.168.42.43 for the IP address, and 255.255.255.0 for subnet mask.
6. Click **OK** and **Close** to exit the dialog box.

For Mac

1. Launch the Apple Menu. Select **System Preferences**. Then click **Network Control Panels** and click **TCP/IP.**
2. Select the network configuration with the green icon lit up from the TCP/IP. This is your active connection. Then click **Configure**.
3. Go to **Ethernet settings**, select **Manually** from the drop-down menu.
4. In the IP Address field, enter 192.168.42.43, and enter 255.255.255.0 in the Subnet Mask field.
5. Click **Apply.**

Appendix b

About MX Records (for Step 10)

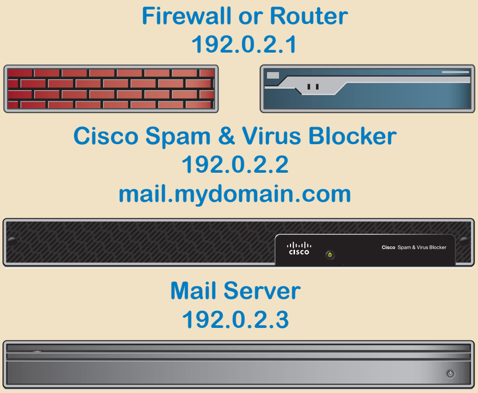
A DNS record is like an entry in an Internet “phone book” for your domain. It translates a hostname (such as example.com) into an IP address. Included in the DNS record is an A record that maps the appliance hostname to its IP address and an MX record that directs incoming email to the correct mail server.

If your MX record routes mail to your email server, you will need to change your MX records to point to your Blocker appliance. If you use a NAT device, you may be able to skip this step (see Appendix C About Network Address Translation).

To change your MX records, locate the MX records on your DNS server. You may have a local DNS server, or your DNS records may be hosted by a DNS provider. The Blocker must be the first hop in your network, so ensure that you configure email to route through the Blocker before any other mail server.

To change your MX records, consult your DNS administrator or your DNS provider documentation.

In the following example, the MX record pointed to the mail server originally, and is modified to point to the Blocker:



Before

A Record: exchange.mydomain.com IN A 192.0.2.3
MX Record: mydomain.com in MX exchange.mydomain.com

After

A Record: exchange.mydomain.com IN A 192.0.2.3
A Record: mail.mydomain.com IN A 192.0.2.2
MX Record: mydomain.com in MX mail.mydomain.com

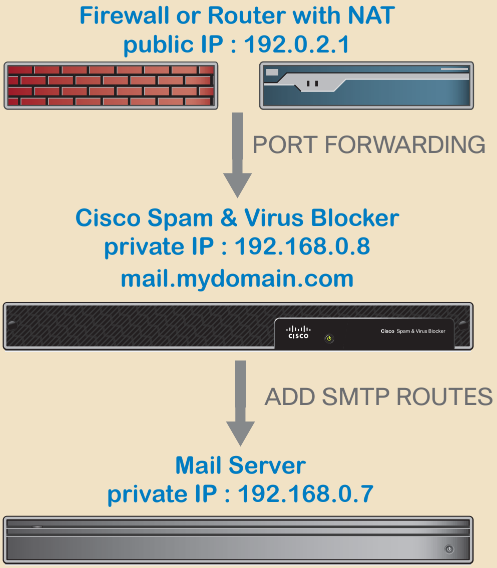
C Appendix

About Network Address Translation (for Step 10)

NAT is the translation of an IP address used within one network to a different IP address used in another network. For example, you might want route email to a public IP address, while keeping all of your other addresses private. If you use Network Address Translation on your router or firewall, you may not need to change your MX records, but you may need to configure port forwarding to ensure email gets routed to the Blocker.

For instructions on changing your NAT translation tables, consult the documentation for your router or firewall.

In this example, the router/firewall uses NAT to route email from the public IP address of 192.0.2.1 to the internal IP address of the mail server at 192.168.0.7. The MX records do not need to be modified, but port forwarding must be changed to route Port 25 traffic to the Blocker.

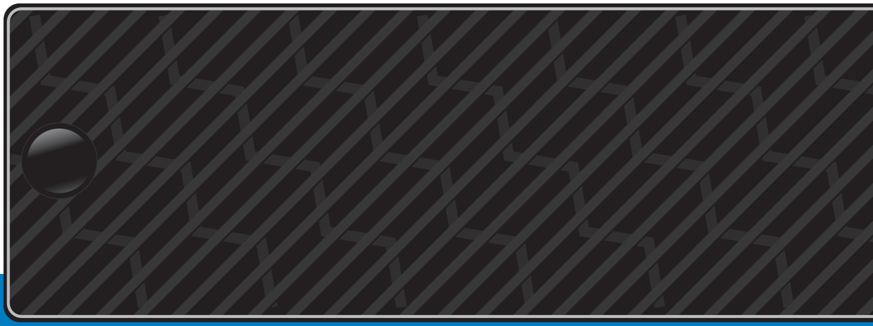


Before

A Record: mail.mydomain.com IN A 192.0.2.1
MX Record: mydomain.com IN MX mail.mydomain.com
Port forwarding: Port 25 traffic to 192.168.0.7

After

A Record: mail.mydomain.com IN A 192.0.2.1
MX Record: mydomain.com IN MX mail.mydomain.com
Port forwarding: Port 25 traffic to 192.168.0.8
SMTP route between Blocker and mail server



Cisco Spam & Virus Blocker
© Cisco 2008
PN 78-18833-01